Université Claude Bernard Lyon 1

MASTER M1G

Algèbre

Fiche TD 1

Exercice 1 *Automorphismes de $\mathbb{Z}/n\mathbb{Z}$*

1. (Question de cours) Montrer que l'application qui, à un élément a de $(\mathbb{Z}/n\mathbb{Z})^*$, envoie l'application $x \mapsto ax$ de $\mathbb{Z}/n\mathbb{Z}$ dans lui-même, définit un isomorphisme du groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^*$ dans le groupe $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ des automorphismes de $\mathbb{Z}/n\mathbb{Z}$. Montrer que son inverse est l'application qui, à ϕ dans $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$, associe $\phi(\overline{1})$.

   Il y a plein de choses à montrer : que l'application est bien (co-)définie, que c'est un morphisme, injectif, surjectif.

2. On suppose que $n := \prod_i p_i^{n_i}$ est la décomposition en facteurs premiers de n. Montrer que l'on a l'isomorphisme de groupes

$$(\mathbb{Z}/n\mathbb{Z})^* \simeq \prod_i (\mathbb{Z}/p_i^{n_i}\mathbb{Z})^*$$

   On se rappelle de la construction de l'isomorphisme du lemme chinois. Pourquoi cet isomorphisme envoie les inversibles sur les inversibles ? Pourquoi le produit direct des inversibles est égal aux inversibles du produit direct ?

3. En déduire une formule pour le nombre $\varphi(n)$ des inversibles de $\mathbb{Z}/n\mathbb{Z}$.

4. Décrire $(\mathbb{Z}/5\mathbb{Z})^*$, $(\mathbb{Z}/9\mathbb{Z})^*$, $(\mathbb{Z}/45\mathbb{Z})^*$. Ce dernier est-il cyclique ?

   Un bon argument pour cette dernière question serait en termes d'exposant du groupe. Un meilleur serait en termes d'unicité de la décomposition des groupes abéliens finis.

Exercice 2 *Automorphismes de $\mathbb{Z}/n\mathbb{Z}$ (suite et fin)*

Le but de l'exercice est de décomposer en groupes cycliques le groupe des automorphismes de $\mathbb{Z}/n\mathbb{Z}$ (qui est abélien par l'exercice précédent). Dans un esprit de modération nous allons nous limiter au cas où $n = p^k$.

1. Trouver un élément d'ordre 6 dans $(\mathbb{Z}/7\mathbb{Z})^*$, un élément d'ordre 12 dans $(\mathbb{Z}/13\mathbb{Z})^*$. Pouvait-on être certain de leur existence ?

2. On veut montrer que $(\mathbb{Z}/p\mathbb{Z})^* \simeq \mathbb{Z}/(p-1)\mathbb{Z}$, c'est-à-dire qu'il existe un élément d'ordre $(p-1)$ dans $(\mathbb{Z}/p\mathbb{Z})^*$.

   (a) Montrer que sur $(\mathbb{Z}/p\mathbb{Z})^*$, le nombre d'éléments d'ordre d est inférieur ou égal à $\varphi(d)$.

(b) A l'aide de l'égalité $n = \sum_{d|n} \varphi(d)$ (que signifie cette égalité ?), conclure qu'il existe forcément un élément d'ordre $p-1$.

3. On suppose que p est premier impair et on veut montrer que $(\mathbb{Z}/p^k\mathbb{Z})^*$ est cyclique.

   (a) Montrer qu'il existe λ_k, pour tout k premier à p tel que

   $$(1+p)^{p^k} = 1 + \lambda p^{k+1}.$$

   (b) Montrer qu'il existe un élément d'ordre $p-1$ dans $(\mathbb{Z}/p^k\mathbb{Z})^*$.

   (c) Montrer qu'il existe un élément d'ordre $p^{k-1}(p-1)$. Conclure.

4. Où s'est-on servi du fait que p était impair ?

Voir solution sur l'autre fiche

Exercice 3 *Produits (semi-)directs internes*

1. On suppose qu'un groupe fini G possède deux sous-groupes distingués H et K tels que
   • $\#H\#K = \#G$,
   • $\#H$ et $\#K$ sont premiers entre eux.
   Montrer que G est isomorphe au produit direct $H \times K$.
   On construit tout d'abord une application de $H \times K$ dans G par multiplication...
2. Que se passe-t-il si seul K est distingué ?
   On pense tout de suite au produit semi-direct.
3. Application : Montrer que le seul groupe d'ordre 15 est cyclique.
   On peut commencer par regarder les Sylow d'un groupe d'ordre 15.
4. Généraliser cette application à un groupe d'ordre pq tel que $q < p$ sont deux nombres premiers, avec p non congru à 1 modulo q.
5. Que se passe-t-il si p est congru à 1 modulo q, par exemple, pour 6 ou $2p$, avec p premier impair ?

Exercice 4 *Nombre de groupes abéliens d'ordre fixé*

1. Combien y a-t-il de groupes abéliens d'ordre p^n avec p premier ? Montrer que ce nombre est égal au terme en z^n dans le produit infini $\prod_{k=1}^{+\infty} \frac{1}{1-z^k}$.
   Le théorème de structure des groupes abéliens finis fait le lien entre ce nombre et le nombre de partitions de n. Pour la dernière question, il faut développer $\frac{1}{1-z^k}$ en votre série préférée (Non, pas Games of Thrones !).
2. Combien y a-t-il de groupes abéliens d'ordre n avec $n = \prod_i p_i^{n_i}$?

Exercice 5 *Réciproque de Lagrange dans le cas abélien fini*

1. Montrer que si G est un groupe cyclique d'ordre n, alors, pour tout diviseur d de n, il existe un unique sous-groupe d'ordre d de G.

   On se ramène au cas où $G = \mathbb{Z}/n\mathbb{Z}$ et on pose $a = n/d$. Le sous-groupe engendré par a fait l'affaire. Pour l'unicité, dire qu'un élément $\overline{k}$ d'un sous-groupe d'ordre d va vérifier $d\overline{k} = \overline{0}$.

2. Quels sont les morphismes entre les groupes additifs $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z}$?

   Analyse-synthèse. Un tel morphisme φ est entièrement déterminé par la donnée de $\varphi(\overline{1})$. Ce dernier doit forcément être annulé par m et par n, donc par leur pgcd, disons, d. Réciproquement, la donnée d'un élément de $\mathbb{Z}/m\mathbb{Z}$ annulé par d fournit un unique morphisme φ de $\mathbb{Z}/n\mathbb{Z}$ vers $\mathbb{Z}/m\mathbb{Z}$.

3. Quels sont les groupes d'ordre 12 ?

   Quel est le rapport avec ce qui précède ? Ah, peut-être les produits semi-directs ?

Exercice 6 *Groupe des isométries du tétraèdre et surjection exceptionnelle $\mathfrak{S}_4 \to \mathfrak{S}_3$.*

Soit G le groupe des isométries du tétraèdre régulier $\mathcal{T}$. On admettra qu'un élément de G envoie un sommet de $\mathcal{T}$ sur un sommet de $\mathcal{T}$.

1. Montrer, en faisant agir G sur l'ensemble des sommets du tétraèdre, que G est isomorphe à $\mathfrak{S}_4$.

   L'action sur l'ensemble des sommets fournit un morphisme de G dans $\mathfrak{S}_4$. Pour l'injectivité, on montrera qu'un élément du noyau fixe un repère de l'espace. Pour la surjectivité, on montrera que les transpositions de $\mathfrak{S}_4$ sont atteintes.

2. En déduire un morphisme surjectif de $\mathfrak{S}_4$ sur $\mathfrak{S}_3$. Quel est son noyau ?

   En gros, la bonne question à se poser est : le groupe G agit sur trois quoi ? Le mieux est d'inscrire le tétraèdre dans un cube de sorte que les trois axes du cube sont les trois bimédianes du tétraèdre. Pour le noyau, on peut commencer à trouver son ordre.

3. Montrer que $\mathfrak{S}_4$ est un produit semi-direct de $\mathfrak{S}_3$ sur $(\mathbb{Z}/2\mathbb{Z})^2$.

Exercice 7 *p-Sylow de $\mathrm{GL}_n(\mathbb{F}_p)$*

1. Soit p un nombre premier. Quels sont les p-Sylow du groupe $\mathrm{GL}_n(\mathbb{F}_p)$?

   Commencer par trouver le cardinal de $\mathrm{GL}_n(\mathbb{F}_p)$. Il y en a autant que de bases de l'espace $\mathbb{F}_p^n$. Montrer que l'ordre d'un p-Sylow est $p^{\frac{n(n-1)}{2}}$. Considérer le sous-groupe U des matrices triangulaires supérieures avec des 1 sur la diagonale.

2. Montrer que le stabilisateur de U pour la conjugaison, est le groupe T des matrices triangulaires supérieures (inversibles).

   Il est assez clair que la conjugaison par T stabilise U. Pour la réciproque, notons E_k le sous-espace engendré par les k premiers vecteurs de la base canonique. On remarque que si g est dans le stabilisateur de U, alors, $g(E_k)$ est stabilisé par U, et que l'on a donc $g(E_k) = E_k$.

3. Combien $\mathrm{GL}_n(\mathbb{F}_p)$ possède-t-il de p-Sylow ?

   Tous les p-Sylow sont conjugués. On est ramené à trouver le cardinal du stabilisateur de U pour la conjugaison, qui se trouve être le groupe T.

Exercice 8 *p-Sylow de $\mathfrak{S}_p$*

1. Soit p un nombre premier. Quels sont les p-Sylow de $\mathfrak{S}_p$? Montrer qu'il y en a exactement $(p-2)!$ En déduire une preuve élégante de la formule de Wilson : $(p-1)!$ est congru à -1 modulo p.
2. Quels sont les Sylow de $\mathfrak{S}_3$, $\mathfrak{S}_4$, $\mathfrak{S}_5$?
   Pour $\mathfrak{S}_3$, on peut tout faire à la main. Mais pour $\mathfrak{S}_4$, il est bien de réaliser $\mathfrak{S}_4$ comme le groupe du tétraèdre régulier. Pour $\mathfrak{S}_5$ et pour les p-Sylow, avec $p \neq 5$, on peut considérer une injection naturelle de $\mathfrak{S}_4$ dans $\mathfrak{S}_5$.
3. Quels sont les normalisateurs de ces Sylow ? (voir tableau)

	S_2	n_2	N_2	S_3	n_3	N_3	S_5	n_5	N_5
$\mathfrak{S}_3$	$\mathbb{Z}/2\mathbb{Z}$	3	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/3\mathbb{Z}$	4	$\mathfrak{S}_3$			
$\mathfrak{S}_4$	D_4	3	D_4	$\mathbb{Z}/3\mathbb{Z}$	4	$\mathfrak{S}_3$			
$\mathfrak{S}_5$	D_4	15	D_4	$\mathbb{Z}/3\mathbb{Z}$	10	$\mathfrak{S}_3$	$\mathbb{Z}/5\mathbb{Z}$	6	$\mathbb{Z}/5\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$

Exercice 9 *Un sous-groupe d'indice premier p minimal est distingué*

Le but de l'exercice est de montrer que si H est un sous-groupe d'indice p de G, avec p premier minimal divisant l'ordre de G, alors H est distingué.

1. En faisant agir G à gauche sur G/H, fournir un morphisme de G dans $\mathfrak{S}_p$.
2. En déduire un morphisme de H dans $\mathfrak{S}_{p-1}$.
   Comme H fixe la classe H de l'élément neutre, il permute les $p-1$ classes restantes.
3. Montrer que ce morphisme $H \to \mathfrak{S}_{p-1}$ est trivial.
   En fait, les ordres de H et de $\mathfrak{S}_{p-1}$ sont premiers entre eux.
4. Conclure.
   On vient de voir que $HgH = gH$ pour tout g de G. Donc, $Hg = gH$.

Exercice 10 *Classification des groupes simples : l'ordre 60*

On veut montrer qu'un groupe simple d'ordre 60 est isomorphe au groupe alterné $\mathfrak{A}_5$.

1. Montrer que si ϕ est un morphisme d'un groupe G vers un groupe H, alors ϕ envoie le groupe dérivé $D(G)$ dans $D(H)$. Que peut-on en déduire d'intéressant si l'on prend pour H un groupe abélien ?
2. Soit G un groupe simple d'ordre 60. Montrer qu'il possède 6 5-Sylow.
3. En déduire qu'il existe un morphisme injectif ϕ de G dans $\mathfrak{S}_6$.
   On fait agir par conjugaison G sur l'ensemble de ses 5-Sylow. Pour l'injectivité, on utilise, d'une part, la simplicité de G, d'autre part, la transitivité de l'action, par le théorème de Sylow.
4. En déduire que G s'injecte dans $\mathfrak{A}_6$. En assimilant G à son image, quel est le cardinal de $\mathfrak{A}_6/G$?

5. Montrer, en faisant agir $\mathfrak{A}_6$ sur l'ensemble des classes $\mathfrak{A}_6/G$, que G s'injecte dans $\mathfrak{S}_5$, puis, dans $\mathfrak{A}_5$.

   L'action de $\mathfrak{A}_6$ sur l'ensemble des classes $\mathfrak{A}_6/G$ est forcément fidèle. Pourquoi ? G fixe la classe du neutre et du coup, s'injecte dans $\mathfrak{S}_5$.

Exercice 11 *Groupe projectif et isomorphismes exceptionnels*

1. Soit $\mathbb{K}$ un corps. On fait agir $\mathrm{GL}_n(\mathbb{K})$ sur l'ensemble des droites (vectorielles) de $\mathbb{K}^n$. Montrer que le noyau de l'action est le sous-groupe des homothéties de $\mathrm{GL}_n(\mathbb{K})$.

   On peut faire le cas $n = 1$ à part. Si $n = 2$, et si on choisit deux vecteurs u et v, alors un élément φ du noyau vérifie $\varphi(u) = \lambda_u u$, $\varphi(v) = \lambda_v v$. Il faut montrer $\lambda_u = \lambda_v$. On fera deux cas, selon si (u, v) est libre ou non. Dans le cas libre, considérer $u + v$.

2. On note dans la suite $\mathrm{PGL}_n(\mathbb{K})$ le quotient obtenu ; il agit donc fidèlement sur l'ensemble des droites de $\mathbb{K}^n$. Montrer que $\mathrm{PGL}_2(\mathbb{F}_2) \simeq \mathfrak{S}_3$ et $\mathrm{PGL}_2(\mathbb{F}_3) \simeq \mathfrak{S}_4$.

   Combien y-a-t-il de droites dans $\mathbb{K}^2$ pour les corps considérés ? Quels sont les ordres des groupes en présence ?

Exercice 12 *Etude des p-groupes*

On fixe un nombre premier p. On appelle p-groupe tout groupe non trivial d'ordre une puissance de p. Pourquoi les étudier de près ?

1. Montrer que le centre d'un p-groupe G est non trivial.

   Faire agir G sur lui-même par conjugaison. Comment reconnaître le centre, en termes d'orbites ? Appliquer la formule des classes.

2. En déduire une réciproque de Lagrange dans le cadre des p-groupes : pour tout diviseur d de l'ordre d'un p-groupe, il existe un sous-groupe d'ordre d.

   On trouve tout d'abord un élément d'ordre p dans $Z(G)$, qui engendre un sous-groupe distingué H d'ordre p. Ensuite, on fait une récurrence sur l'ordre du p-groupe G, en considérant la surjection canonique $G \to G/H$.

3. On suppose que G est un groupe, de centre $Z(G)$, tel que $G/Z(G)$ est cyclique. Montrer que G est abélien.

   Considérer deux éléments b et c de G et écrire leurs classes en fonction d'un générateur $\overline{a}$ de $G/Z(G)$. Montrer alors que $bc = cb$.

4. En déduire que tout groupe d'ordre p^2 est abélien. Quels sont les groupes d'ordre p^2 ?

5. Montrer que le groupe des matrices triangulaires supérieures sur $\mathbb{F}_p$, avec des 1 sur la diagonale, est d'ordre p^3 non abélien. Quel est son centre ? Quel est le quotient par le centre ? Peut-on le voir comme un produit semi-direct ?

Exercice 13 *Le groupe H_8*

Le groupe H_8 peut être défini, entre autres [1], comme le 2-Sylow de $\mathrm{SL}_2(\mathbb{F}_3)$.

1. De façon plus traditionnelle, c'est le sous-groupe des matrices entières de SU(2).

1. Décrire le groupe H_8.
   Quel est le cardinal de $\mathrm{GL}_2(\mathbb{F}_3)$*, celui de* $\mathrm{SL}_2(\mathbb{F}_3)$ *? Quel(s) est(sont) son(ses) élément(s) d'ordre* 2 *? Montrer que les éléments d'ordre* 4 *ont pour polynôme caractéristique* X^2+1*, puis, les trouver tous.*
2. Montrer l'isomorphisme $\mathrm{SL}_2(\mathbb{F}_3) \simeq H_8 \rtimes \mathbb{Z}/3\mathbb{Z}$.
   Montrer d'abord que $\mathrm{SL}_2(\mathbb{F}_3)$ *possède un unique* 2*-Sylow.*